Ian Lee

Hw 3

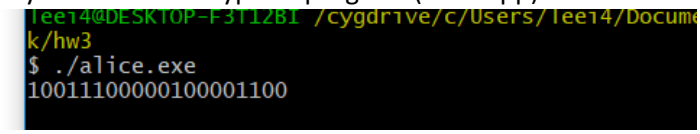
Writeup

1) What is the ciphertext?
   The ciphertext is 00100000110011100100

2) Verify your answer by showing that D(c(m)) = m.

   Original message m is 10011100000100001100

   If you run the decryption program (Alice.cpp) this is the result, which are equal.



   Firstly Alice generates two values p and q, which are prime and are both congruent to 3 mod 4. In this case the p and q values are given as p = 499 and q = 547. Alice then calculates her N which is the public key by multiply p and q such that n = p*q. Alice can then pass N to Bob. When Bob wishes to send a message to Alice he will encode the message as a string of L bits, in binary. Bob then selects a random element r and uses it to compute $X_0 = r^2$ mod N. In our case X_0 is given to us as 159201. Bob then finds the least random bits of a sequence $x_i = x_{i-1}$^2 mod N and then XOR'ing that to obtain the ciphertext. Bob repeats this process until he reaches the end of m, appending the value to the ciphertext each time. Bob will then send Alice the ciphertext, and the last x_i value.

   For decryption Alice will compute d1 and d2 which will allow us to determine the X_0 value chosen by Bob. Using the X_i raised to the d1 or d2 mod N will return values that allow us to determine what X_0 is. Finally we do the same thing that Bob does, and solve for $X_i=X_{i-1}$^2 mod n and then XOR'ing the least bits of that value with the ciphertext to get our original message.